EXHIBIT B

Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks

L.T. Heberlein, B. Mukherjee, K.N. Levitt

Computer Security Laboratory
Division of Computer Science
University of California
Davis, Ca. 95616

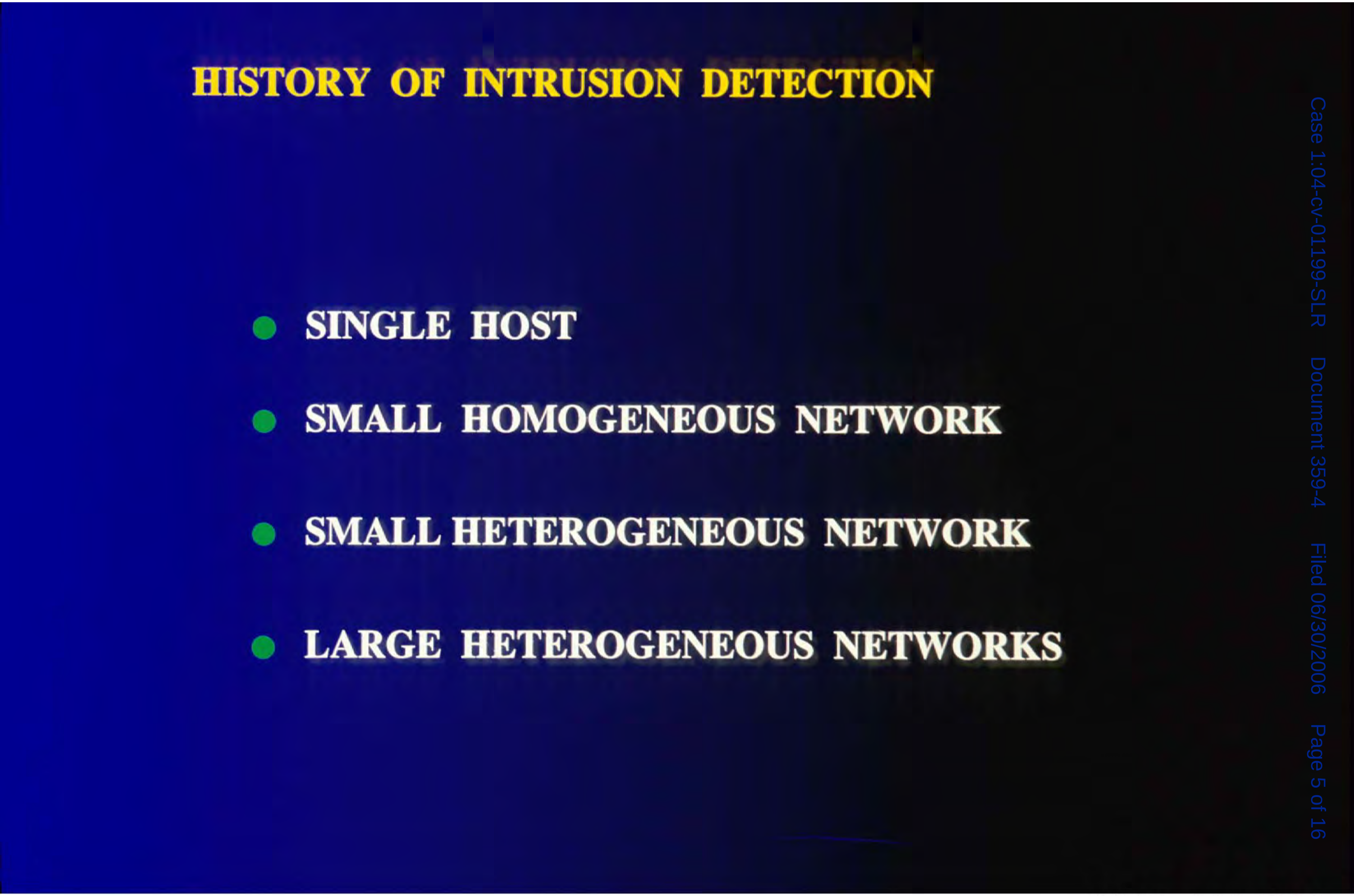
WHY INTRUSION DETECTION?

- FLAWS IN OS DESIGN
- FLAWS IN OS IMPLEMENTATION
- ADMINISTRATIVE ERRORS
- USER ERRORS
- STOLEN PASSWORDS
- SYSTEM COMPLEXITY

INTRUSION DETECTION GOALS

WE WOULD LIKE TO DETECT ACTIVITIES LEADING TO:

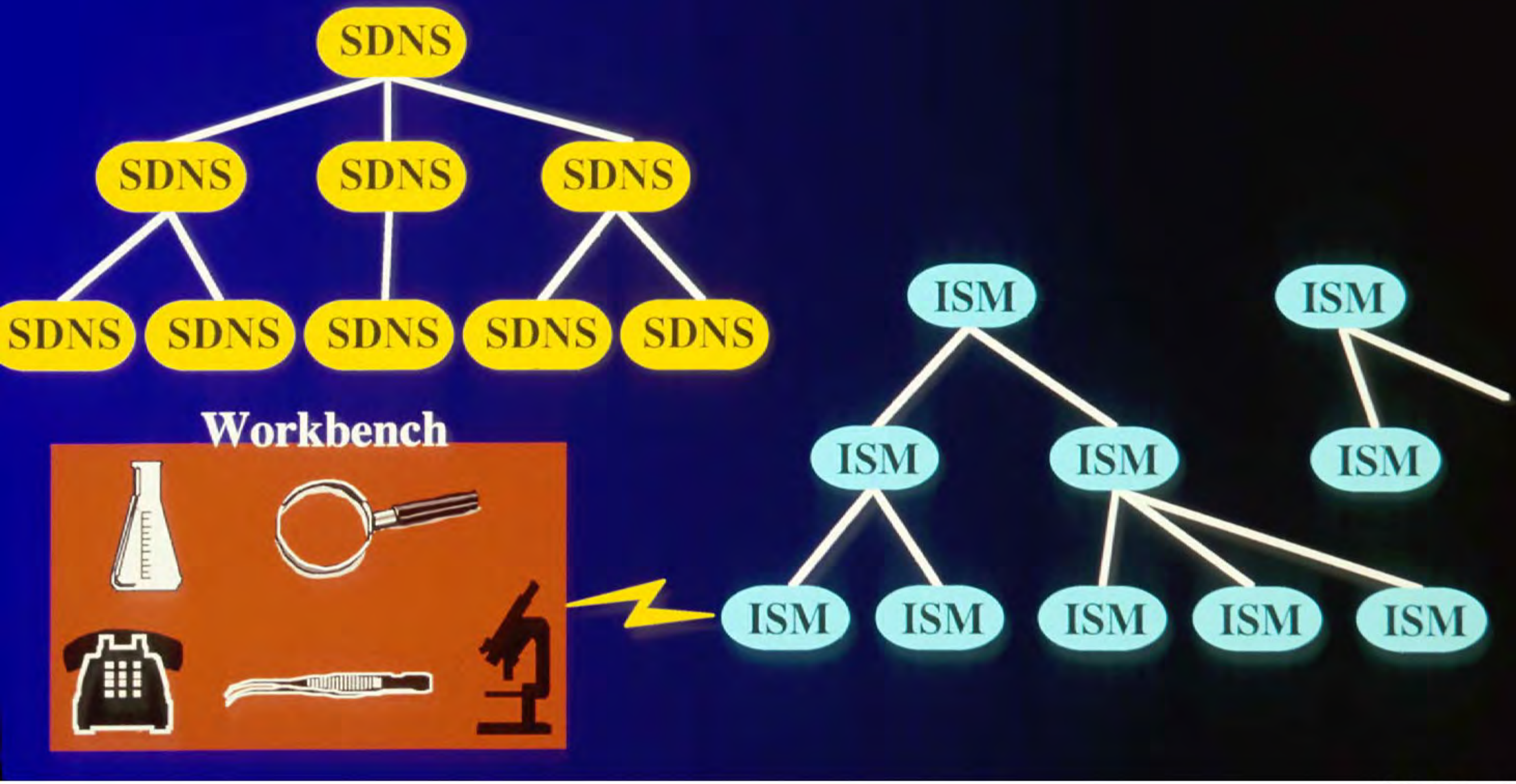
- DISCLOSURE OF INFORMATION
- MODIFICATION OF INFORMATION
- DENIAL OF SERVICE
- ILLEGITIMATE USE OF RESOURCES



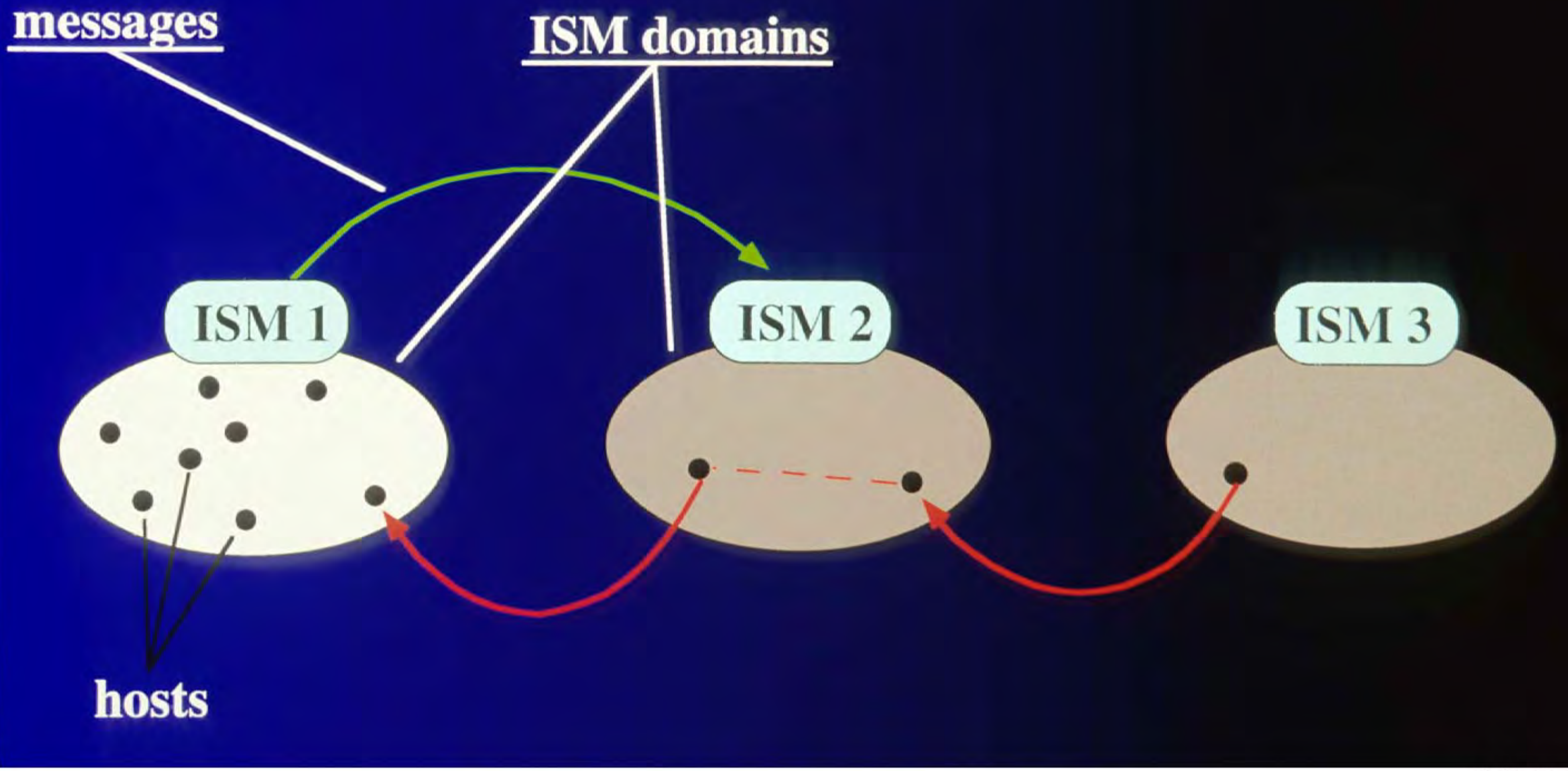
HISTORY OF INTRUSION DETECTION

- SINGLE HOST
- SMALL HOMOGENEOUS NETWORK
- SMALL HETEROGENEOUS NETWORK
- LARGE HETEROGENEOUS NETWORKS

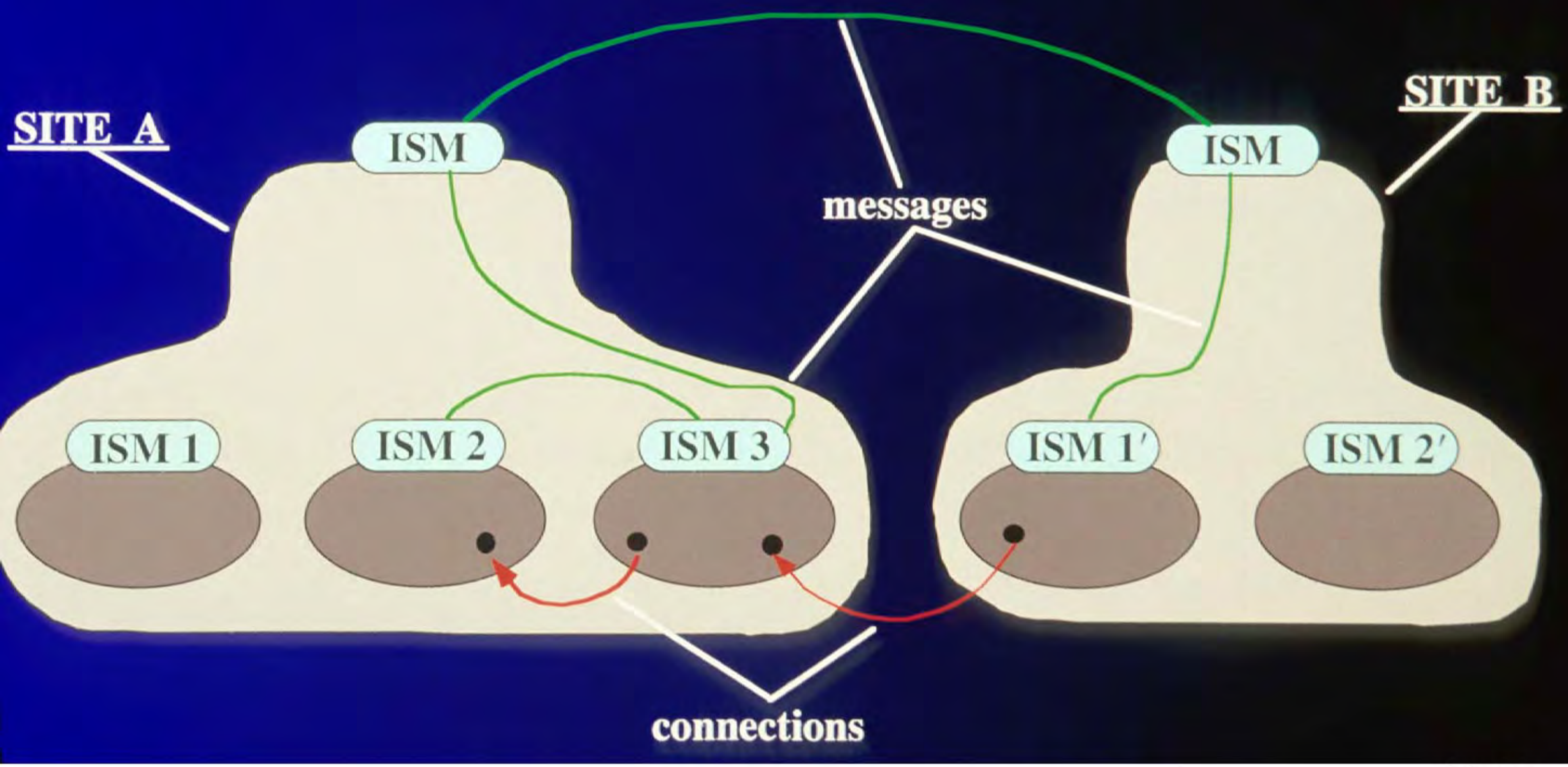
ARCHITECTURE OVERVIEW



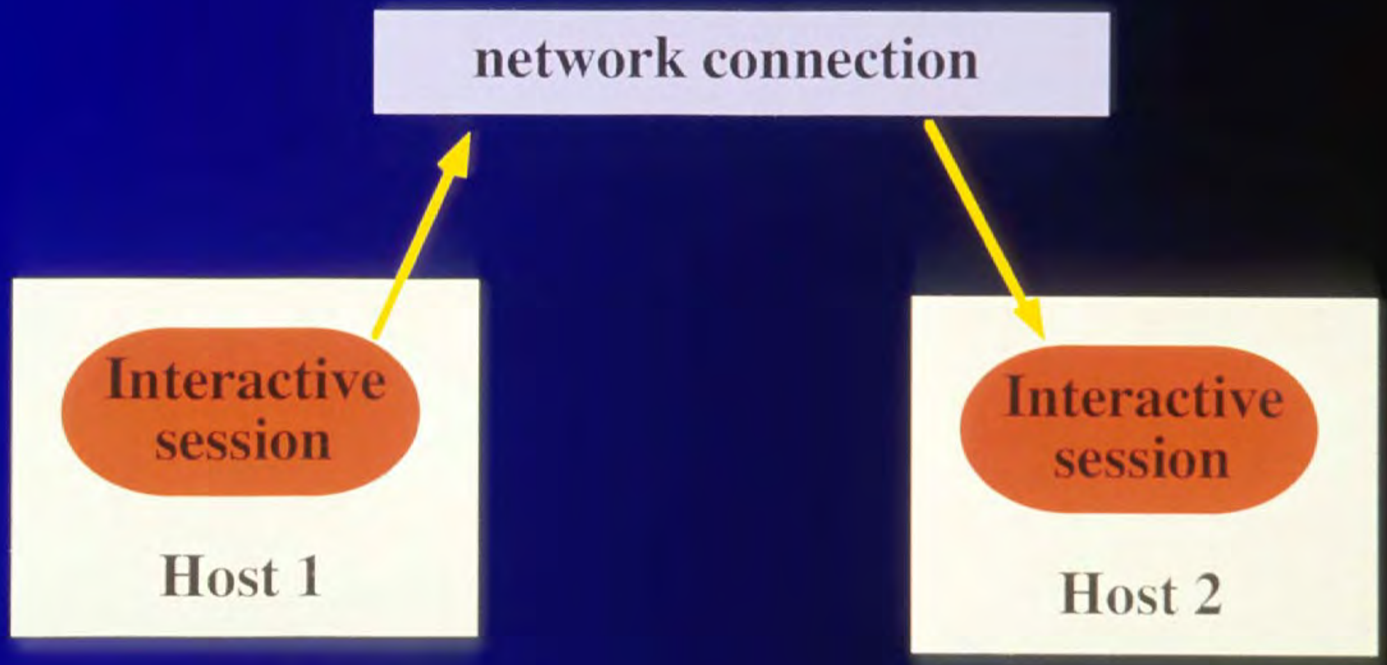
ISM SECURITY DOMAINS



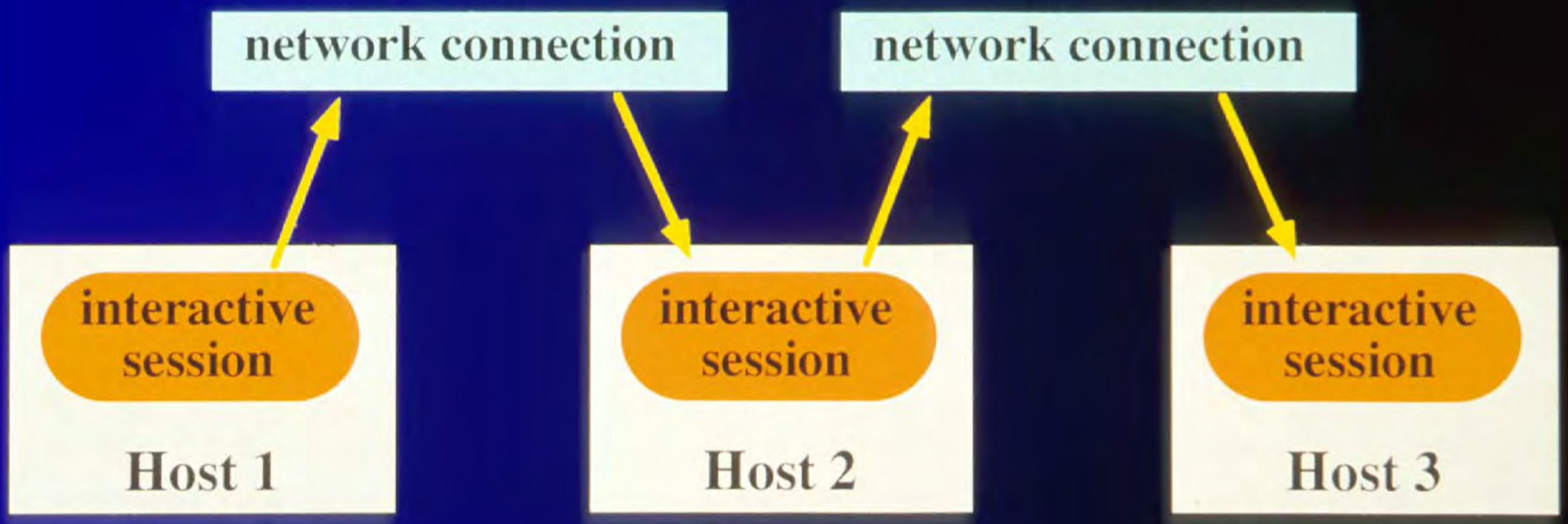
SECURITY DOMAIN HIERARCHY



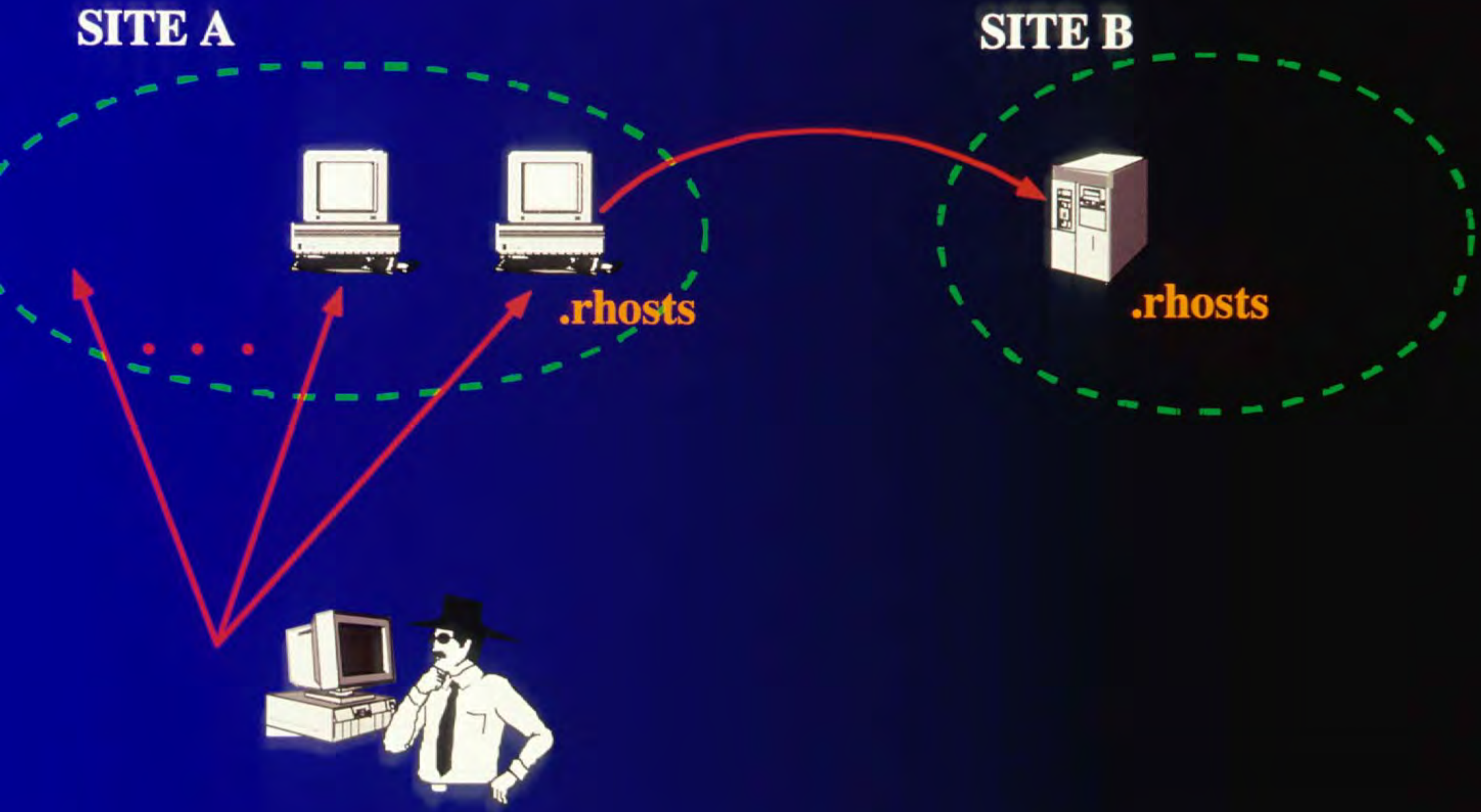
NETWORK CONNECTION AS A SHARED RESOURCE



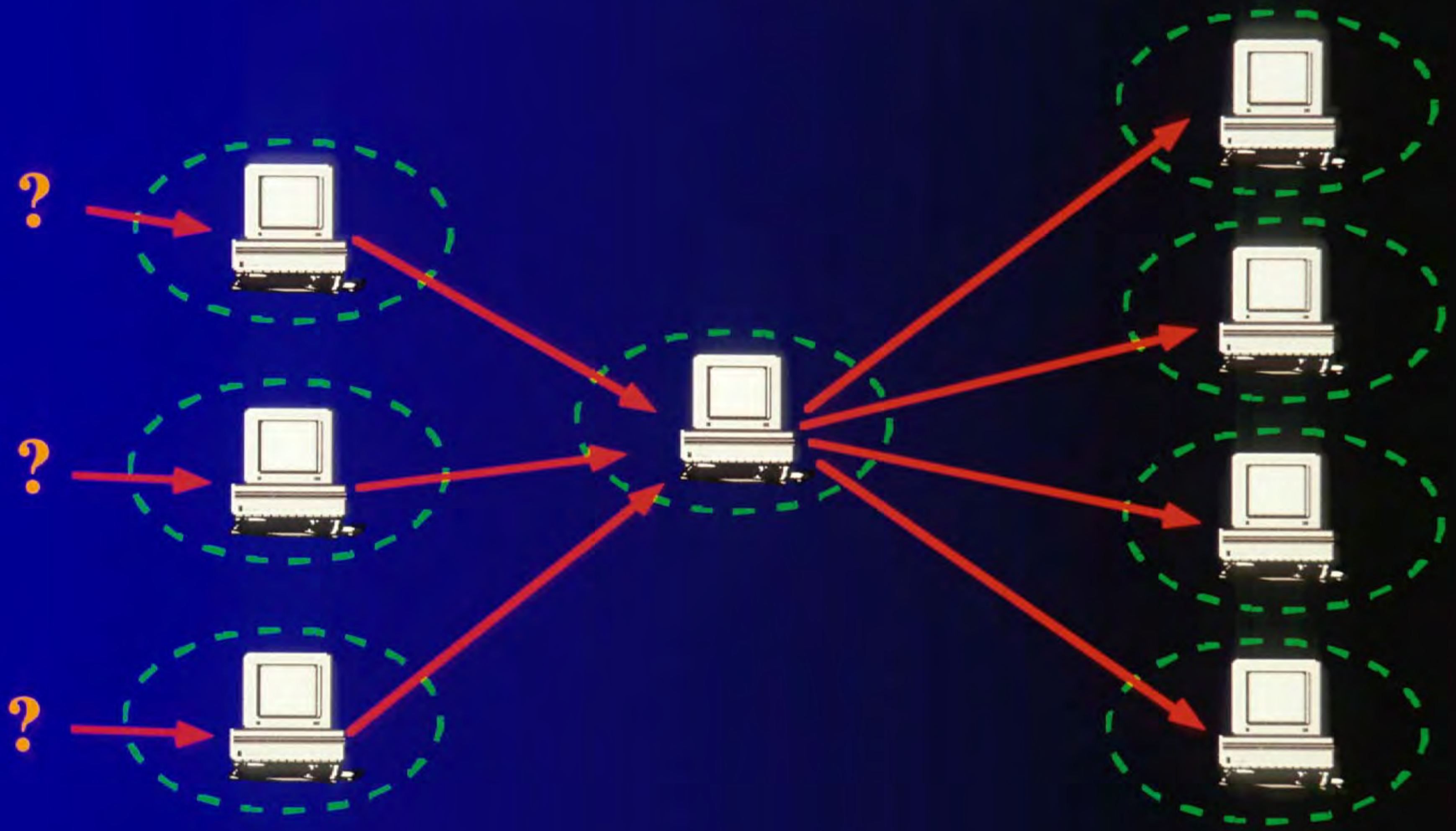
MULTIPLE HOPS ACROSS THE NETWORK



SCENARIO: ABUSING TRUST



SCENARIO: UNKNOWN SOURCE



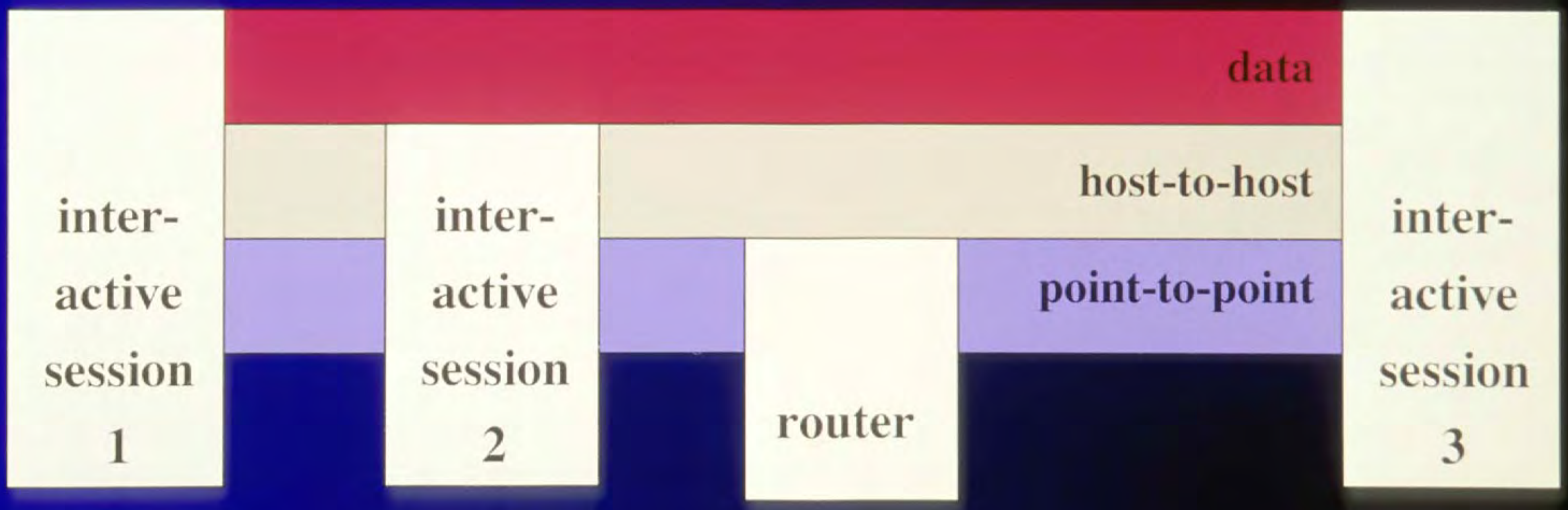
ACCOUNTABILITY

- WHO ARE YOU?
  WHAT ARE YOU DOING?
- ACCOUNTABILITY ACROSS OS BOUNDARY
- NETWORK IDENTIFIER

THUMBPRINT GOALS

- RESOLUTION
- SEMANTIC FREE
- EFFICIENCY

EXTENDED NETWORK CONNECTION



inter-active session 1

inter-active session 2

router

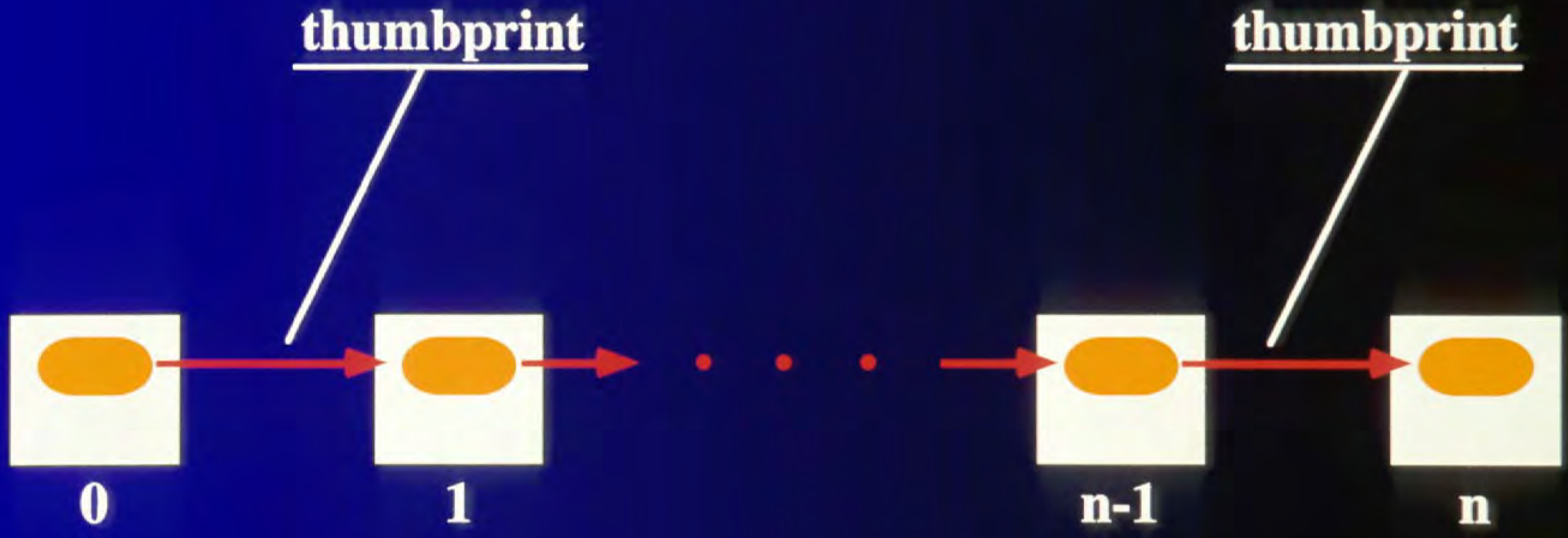
inter-active session 3

data

host-to-host

point-to-point

TRACKING A USER ACROSS UNMONITORED HOSTS


thumbprint
thumbprint
0
1
n-1
n